

Philip J. Berg, Esquire (PA I.D. 9867)
E-mail: philjberg@gmail.com
LAW OFFICES OF PHILIP J. BERG
555 Andorra Glen Court, Suite 12
Lafayette Hill, PA 19444-2531
Telephone: (610) 825-3134 Fax: (610) 834-7659
Attorney in pro se and for Plaintiffs

**UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA,
SOUTHERN DIVISION**

LISA LIBERI, et al,

Plaintiffs,

vs.

ORLY TAITZ, et al,

Defendants.

CIVIL ACTION NUMBER:

8:11-cv-00485-AG (AJW)

**DECLARATION OF PHILIP J.
BERG, ESQUIRE**

Date of Hearing: December 19, 2011
Time of Hearing: 10:00 a.m.
Location: Courtroom 10D

DECLARATION OF PHILIP J. BERG, ESQUIRE

I, Philip J. Berg, Esquire, am over the age of 18 and am a party to the within action. I have personal knowledge of the facts herein, and if called to do, I could and would competently testify. I am making this Declaration under the penalty of perjury of the Laws of the United States pursuant to 28 U.S.C. §1746.

1. I am an Attorney in good standing, licensed to practice law in the Commonwealth of Pennsylvania. I am licensed to practice in the U.S. District

1 Courts, Middle and Eastern District of Pennsylvania; Third Circuit Court of
2 Appeals; the Pennsylvania Supreme Court; and the U.S. Supreme Court.

3
4 2. Defendant Orly Taitz threatened to take me down and to do so she was
5 going to destroy my Paralegal, Plaintiff Lisa Liberi and get rid of her. Defendant Orly
6 Taitz was successful in destroying Plaintiff Lisa Liberi.

7
8 3. Defendant Orly Taitz also set out to destroy Plaintiff Lisa Ostella because
9 Plaintiff Lisa Ostella refused to lie and falsify information in order to substantiate
10 Defendant Orly Taitz's false statements, false claims and lies pertaining to "hacking",
11 "cracking", and theft of donated money and of her (Taitz's) website.

12
13 4. This case is **not** about any type of "intra-Birther Movement feud", nor is it
14 a "politically motivated skirmish". This case is about Defendant Orly Taitz's threats
15 against me and the Plaintiffs Lisa Liberi ["Liberi"] and Lisa Ostella ["Ostella"]. The case
16 against Daylight Chemical Information Systems, Inc. and Yosef Taitz is due to their
17 assistance to Defendant Orly Taitz in access to and gaining of Plaintiffs private data,
18 without the knowledge and/or permission of the Plaintiffs, in carrying out her threats
19 against the Plaintiffs.
20

21
22 5. Private data includes but is **not** limited to full Social Security
23 numbers, dates of births, spouses private data, places of birth, maiden names,
24 mother's maiden names, financial records, credit reports, consumer reports,
25 background checks, medical information, sealed court case information, adoption
26
27
28

1 records, Plaintiffs children's information, etc., including all of Plaintiffs primary
2 identification information.

3
4 6. Daylight Chemical Information Systems, Inc. ["Daylight"] brings
5 forth in their Motion to Dismiss ["MTD"] that Daylight's products are for the
6 "chemical" purpose. As pled in Plaintiffs First Amended Complaint ["FAC"]
7 Daylight is a **software development company**, **Not a chemical company**. Their
8 scripts are **not** indigenous to the pharmaceutical industry. Anything can be
9 inserted into the 'quotes', but displaying their scripts with chemical equations
10 ensures their applications will appear more complicated to hide the true
11 functionality of their programs.
12
13
14

15 7. As explained in Plaintiffs FAC, Daylight's applications are in the
16 architecture of Oracle and reach further with other software components developed
17 under Daylight, Twilight LLC, MetaMorphics LLC, ChemoInformatics and other
18 affiliates. This gave Daylight back door access to the Intelius and Reed
19 Defendants databases. This is especially true with systems that are partners; such
20 as, Oracle, Sun Microsystems, MDL Elsevier, universities, pharmaceutical
21 companies, the Reed Defendants and more.
22
23
24

25 8. Contrary to Daylight's statements in their MTD, Daylight has always
26 been well aware of the dual purpose of their software and scripts. Their shared
27 tool server and libraries are scripted for **Global Access**:
28

1 \$DY_ROOT/lib

2 \$DY_ROOT/bin

3
4 9. As shown in Daylight's scripting and manuals, filed with this Court as
5 Exhibits "141" (DCIS Cartridge); "142" (DCIS' fingerprinting); "143" (DCIS Dual
6 Purpose Manual); and "144" (DCIS DayCart) appearing in Docket Entry Numbers 190-
7 26 and 190-27, and as pled in Plaintiffs FAC, the Dollar sign in their code scripting
8 indicates Global Access. The dollar sign is called Sigil in programming.
9 Understanding a program with Global Access requires knowledge about the
10 context and hidden abilities. Understanding the access creates a pipeline into a
11 program from the root that allows registry access and editing. Daylight is well
12 aware of these hidden abilities in their programs. Understanding the use of Sigil
13 Variables entails understanding a large portion of the software program. Daylight
14 held 'hacker classes' with their 'krewe' monthly, for years.

15
16 10. Daylight's access to database servers, running programs internally
17 could alert remote access to IT personnel of unauthorized access and functions, if
18 the proper security is in place. But, having Neil Sankey and The Sankey Firm run
19 information requests created a hard link to compiled information that was easier to
20 take from the Reed and Intelius Defendants systems.
21
22
23
24
25
26
27
28

1 11. Information on the tools that make these functions possible for
2 Daylight, and that are embedded within the architecture of servers like Oracle are
3 located in their manuals on their website at
4 <http://www.daylight.com/products/toolserver.html>.
5

6 12. The Remote Toolkit consists of a server that locally processes all
7 Daylight Toolkit functions for a remote client. For the cost of network overhead,
8 toolkit clients share the toolkit server's resources, e.g., CPU power, shared
9 programs, databases, etc. In general, hardware and operating systems supplied
10 with PC's and Macintoshes cannot efficiently handle the high-performance
11 methodology of Daylight algorithms. A low-cost Macintosh or PC client may be
12 connected to a remote toolkit server on a more powerful Unix workstation. As an
13 example, a SMILES might be entered into a Macintosh which would send it to a
14 Unix machine to be interpreted; the Macintosh might then request database
15 searching and depiction generation via the Unix machine for display on the
16 Macintosh.
17

18 13. The programming environment is identical to local toolkit
19 programming with the addition of two functions to connect to and disconnect from
20 the toolkit server.
21
22
23
24
25
26
27
28

1 14. Programs written with the Remote Toolkit will **not** operate in a stand-
2 alone environment (a Remote Toolkit Server must be accessible over an IP
3 network).
4

5 15. All Daylight Toolkit functions are supported by the 4.5 Remote
6 Toolkit. The Remote Toolkit server (daytoolserver) is available on all supported
7 Unix platforms. Only the client side of the remote toolkit exists on personal
8 computers, available for Macintosh (via MacTCP) and PC/Windows (via
9 WinSockets).
10
11

12 16. Also in the Toolkit is The Conversion Toolkit which is aimed at
13 facilitating migration of data into and out of Daylight software.
14

15 17. Defendants Yosef Taitz by and through Daylight used Daylight's
16 tools outlined herein to access Plaintiffs private data from the Reed and Intelius
17 Defendants databases, computers and servers. Yosef Taitz utilized his skills,
18 access, and job functions that he uses in his line of employment with Daylight.
19

20 18. All the information herein is pled in Plaintiffs FAC and explained in
21 Exhibits "141" through "144" appearing as Docket Entry Numbers 190-26 and 190-
22 27. This is how Yosef Taitz through DCIS was able to access Plaintiffs private data, that
23 Mr. Taitz through his Corporation, Daylight provided to Defendant Orly Taitz. With the
24 private data of Plaintiffs, Defendant Orly Taitz carried out her threats of harm towards
25 the Plaintiffs. As a result, Plaintiffs suffered severe damages.
26
27
28

19. Defendant Orly Taitz published all the private data of Plaintiffs that she received from the Sankey Defendants, her husband, Yosef Taitz by and through and with the use of Defendant Daylights tools, the Reed and Intelius Defendants through the Internet, mass emailing, postal mailings, RSS feeds, repeatedly, including sending it internationally. All of which caused Plaintiffs severe serious damages. Defendant Orly Taitz could **not** have completed her goal in destroying the Plaintiffs had the Defendants **not** made Plaintiffs private data available, accessible, and provided the information to her. This includes Daylight.

I declare under the penalty of perjury of the Laws of the United States and California that the foregoing is true and correct.

Executed this 23rd day of November, 2011 in the Commonwealth of
Pennsylvania, County of Montgomery.

/s/ Philip J. Berg

Philip J. Berg, Esquire, Declarant